Zał. nr 4 do Polityki

PROCEDURA ANALIZY RYZYKA

Celem procedury jest opisanie zasad przeprowadzenia analizy ryzyka, która w efekcie ma doprowadzić do zastosowania odpowiednich dla Administratora środków technicznych i organizacyjnych zapewniających obniżenie ryzyka przypadkowego lub niezgodnego z prawem zniszczenia, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

Artykuł 24 RODO opisuje jeden z obowiązków Administratora Danych i brzmi następująco;

„Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane."

Każdy Administrator Danych ma więc obowiązek przeprowadzenia analizy ryzyka, żeby ustalić jego poziom w stosunku do różnych aktywów uczestniczących w przetwarzaniu. Podstawowym aktywem, którym zajmuje się RODO są dane osobowe, które należą do kategorii informacji.

W kontekście bezpieczeństwa informacji bierze się pod uwagę następujące atrybuty:

- integralność – właściwość zapewniająca, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany,

- poufność – właściwość zapewniająca, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom,

- dostępność – właściwość zapewniająca, że dane są dostępne zgodnie z wymaganiami użytkownika.

Wartość ryzyka (R) wylicza się według poniższego wzoru dla każdego z atrybutów bezpieczeństwa.

R = P * S

gdzie : P – prawdopodobieństwo wystąpienia zagrożenia

S – Szkodliwość skutków zmaterializowania się zagrożenia (wartość aktywa)

Sumaryczne ryzyko zmaterializowania się zagrożenia jest wyliczane według wzoru:

R = Ri + Rp +Rd

gdzie Ri – ryzyko utraty integralności

Rp – ryzyko utraty poufności

Rd – ryzyko utraty dostępności

Analizę ryzyka przeprowadza się w następujących krokach:

1. Identyfikacja aktywów biorących udział w przetwarzaniu, w tym danych osobowych i oszacowanie skutków zmaterializowania się zagrożenia.

Przykładowe aktywa to zbiory danych osobowych, informacje uwierzytelniające, sprzęt komputerowy, usługi, w tym outsourcing, budynek. Aktywa można odpowiednio pogrupować.

Każde aktywo lub grupę aktywów należy wycenić przez pryzmat skutku zmaterializowania się zagrożenia. W jakościowej metodzie analizy ryzyka przyjmuje się, że wartość aktywa (S) jest wyrażone liczbą z przedziału 1-3, gdzie:

1 – zdarzenie wywołuje niewielki skutek (np. czas niedostępności informacji jest stosunkowo krótki, cena odtworzenia aktywa w przypadku utraty nie jest wysoka, utrata poufności dotyczy niewielkiej ilości danych),

2 – zdarzenie wywołuje znaczący skutek (np. czas niedostępności informacji lub usług systemu jest odczuwalny, cena odtworzenia aktywa jest dość wysoka, utrata poufności dotyczy szczególnych kategorii danych),

3 – zdarzenie wywołuje bardzo znaczący skutek (np. czas niedostępności jest długi i przywrócenie dostępu wiąże się z dodatkowymi kosztami, odtworzenie aktywa jest niemożliwe, utrata poufności wiąże się z koniecznością zawiadomienia Urzędu ochrony danych lub opublikowania informacji w prasie).

2. Identyfikacja zagrożeń, określanych jako potencjalne naruszenie zabezpieczenia systemu informatycznego, które będą uwzględniane w procesie analizy ryzyka.
   Źródłem zagrożeń mogą być:
   - siły wyższe np. klęski żywiołowe,
   - działania przestępcze, w tym:
     - zagrożenia związane z kradzieżą sprzętu, oprogramowania, dokumentów,
     - nieuprawnione działanie personelu,
     - nieuprawnione działanie osób postronnych,
   - błędy personelu obsługującego dokumenty tradycyjne lub system komputerowy,
   - zła organizacja pracy w tym błędy w ochronie fizycznej i technicznej,
   - awarie i uszkodzenia sprzętu i infrastruktury teleinformatycznej.

3. Szacowanie ryzyka zmaterializowania się zagrożeń dla zidentyfikowanych aktywów w kontekście wymienionych wyżej atrybutów bezpieczeństwa z zastosowaniem wzoru
   $R = P * S$
   gdzie prawdopodobieństwo zmaterializowania się zagrożenia przyjmuje wartości:
   1 – niskie
   2 – średnie
   3 - wysokie

   Poziom ryzyka dla poszczególnych aktywów może przyjmować wartości z przedziału 1-27.

4. Wyznaczenie poziomu ryzyka, które akceptujemy.

5. Dla wszystkich zagrożeń w stosunku do których poziom ryzyka jest wyższy - określenie i wdrożenie odpowiedniego postępowania z ryzykiem. Przez postępowanie z ryzykiem rozumie się:
   - przeniesienie ryzyka na stronę trzecią np. outsourcing usług,
   - unikanie ryzyka np. eliminacja procesów lub działań powodujących ryzyko np. zakaz wynoszenia laptopów poza teren firmy,
   - redukcję – zastosowane zabezpieczeń technicznych i organizacyjnych w celu obniżenia ryzyka np. zaszyfrowanie dysków laptopów.

Na podstawie podjętych decyzji powstaje **Plan postępowania z ryzykiem**, który zawiera:
- wybrane warianty postępowania z ryzykiem,
- lista zabezpieczeń do wdrożenia,
- terminy realizacji,
- osoby odpowiedzialne za wdrożenie,
- ewentualne koszty.

Ponowna analiza ryzyka powinna być przeprowadzana cyklicznie, w wyznaczonych odstępach czasu lub po znaczących zmianach w procesie przetwarzania danych osobowych.